UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
7914 SE Evergreen Highway, Vancouver, WA98664 et al., as more fully described in Attachments A-1 and A-2

Case No. MJ21-5081

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachments A-1 and A-2, which are incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
26 U.S.C. § 7206(1)-(2)	False and Fraudulent Statements by Taxpayer; Aiding False and Fraudulent Statements by Third Parties; Wire Fraud
18 U.S.C. § 1343	

The application is based on these facts:

✓ See Affidavit of IRS SA Christian D. Martin continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☑ telephonically recorded.

Christian D. Martin
Applicant's signature

Christian D. Martin, IRS Special Agent
Printed name and title

◯ The foregoing affidavit was sworn to before me and signed in my presence, or
◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 4/15/21

Judge's signature

City and state: Tacoma, Washington

J. Richard Creatura, Chief United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Christian D. Martin, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Internal Revenue Service ("IRS"), Criminal Investigation, and have been since September 2001. My current assignment is to conduct and assist in investigations of various white-collar crimes, including tax fraud, tax-related fraud, and identity theft. My training and experience includes completion of the basic training requirements for a Special Agent at the Federal Law Enforcement Training Center and participation in numerous investigations, during the course of which I have interviewed suspects and witnesses, executed court-authorized search and arrest warrants, and used other investigative techniques to secure relevant information. As a result of my training and experience, I am familiar with techniques and methods used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search the residence located at 7914 SE Evergreen Highway, Vancouver, Washington 98664 (hereinafter "PREMISES I") and premises located at 3312 E Fourth Plain Boulevard, Suites 110 and 115, Vancouver, Washington 98661 (hereinafter "PREMISES II" and, together with PREMISES I, the "SUBJECT PREMISES"), as more fully described in Attachments A-1 and A-2 to this Affidavit, for the property and items described in Attachment B to this Affidavit, as well as any digital devices or other electronic storage media located therein.

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of cooperating

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

witnesses; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits and instrumentalities of violations of Title 26, United States Code, Section 7206(1) (False and Fraudulent Statements by Taxpayer), Title 26, United States Code, Section 7206(2) (Aiding False and Fraudulent Statements by Third Parties), and Title 18, United States Code, Section 1343 (Wire Fraud) will be found at the SUBJECT PREMISES.

SUMMARY OF INVESTIGATION[1]

Initial Steps

5. I became aware of KEITH MARK ALTAMIRANO after coming across a copy of a tax return seemingly prepared by him in the search warrant evidence of an unrelated tax return preparer investigation. The tax return was a 2015 Form 1040, U.S. Individual Income Tax Return, for taxpayer CG ("CG1040"). CG1040 contained questionable Schedule A itemized deductions as the deductions for business mileage, meals and other business expenses exceeded $18,000 but the total income reported was

[1] Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *IP address*. The Internet Protocol address (or simply "IP address") is a unique numeric address used by digital devices on the Internet. Every digital device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that digital device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some digital devices have static—that is, long-term—IP addresses, while other digital devices have dynamic—that is, frequently changed—IP addresses.

b. *Internet*. The Internet is a global network of digital devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. *Storage medium*. A storage medium is any physical object upon which data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

only $21,988. Unreimbursed employee business expenses ("UEBEs") are miscellaneous itemized deductions ("MIDs") that can be deducted by employees on their respective Schedules A, Itemized Deductions, attached to their Form 1040. UEBEs must be paid or incurred during the year for carrying on their trade or business of being an employee and ordinary and necessary. Additionally, MIDs are subject to a two percent (2%) limit, so the deduction is calculated by adding together all MIDs and subtracting from that total two percent (2%) of one's adjusted gross income. Expenses for commuting to work from home and vice versa are not deductible as UEBE.

6. Additionally, CG1040 appeared to be prepared using a consumer version of Turbo Tax, a popular tax preparation software. I know from my training and experience that Turbo Tax will print the phrase, "Self-Prepared" on the line where a paid preparer's firm name would normally be printed. CG1040 had the "Self-Prepared" phrase printed on the line for "Firm's name" but over top of that was a stamp which contained ALTAMIRANO's name, address, and Preparer Tax Identification Number ("PTIN").[2] I searched IRS databases and determined the copy of CG1040 filed with the IRS was filed as a paper return and self-prepared, meaning there were no indications that ALTAMIRANO identified himself as the return preparer on the copy of CG1040 submitted to the IRS.

7. On October 19, 2020, I requested that the IRS Scheme Development Center ("SDC"), which reviews and analyzes tax returns for fraudulent refund schemes, prepare an analysis on return preparer ALTAMIRANO. Because ALTAMIRANO did not sign many of the returns, neither I nor IRS employees at the SDC could search tax returns for ALTAMIRANO's identifying information. Instead, the SDC and I attempted to identify the returns that had been prepared by ALTAMIRANO on the basis of other information; specifically: (a) the email addresses associated with electronically-submitted tax returns;[3]

---

[2] Anyone who prepares or assists in preparing federal tax returns for compensation must have a valid PTIN before preparing returns.

[3] When electronically submitting a Federal Income Tax return to the IRS, taxpayers and preparers have the option to input an email address so that they may receive notifications about their returns via email.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

(b) the IP addresses associated with electronically-submitted tax returns; (c) the Device identification number ("Device ID") associated with the electronically-submitted tax returns;[4] and (d) phone numbers listed on all returns whether filed electronically or mailed.

8. On November 5, 2020, I received the Lead Analysis Results ("LAR") from the SDC. The LAR, combined with my own independent search of IRS databases, identified 1,677 Federal Income Tax returns for tax years 2015-2019 that shared one or more of the queried criteria. The combined analysis also indicated that ALTAMIRANO did not list his name, firm's name, address, employer identification number ("EIN"), or PTIN on 1,540 of the returns (92%) as the paid preparer. When a third-party tax preparer creates and files a tax return on behalf of a taxpayer, the tax preparer is required to list on the return his/her name or his/her tax-preparation firm's name, as well as his/her phone number and address. A tax preparer is also required to list on the return his/her PTIN and/or his/her firm's EIN. In my experience and expertise, I am aware that in other schemes by tax preparers to defraud a taxpayer and/or the federal government, the tax preparer does not ordinarily provide his/her own identifying information on the return. By failing to provide his/her identifying information, the tax preparer attempts to evade detection and liability for false information that may be set out in the return.

The Subject Premises

Premises I

9. On March 16, 2021, ALTAMIRANO was interviewed by an IRS Revenue Agent ("RA") regarding audited tax returns that he prepared. ALTAMIRANO told the RA he has been separated from his wife since 2015 and lives at 2515 Harney Street ("Harney House") in Vancouver, WA. County records confirm ALTAMIRANO owns

[4] The IRS implemented a Device ID field for electronic return filers and preparers for processing year 2015 (generally tax returns prepared for tax year 2014). The Device ID should contain unique data, accessed and transmitted by the software used to create the electronic return, which will identify the specific computer from which the tax return was electronically filed. The Device ID field was voluntary for processing year 2015 but became mandatory for processing year 2016. This means that all returns submitted in processing year 2016 will contain the Device ID and some returns submitted for processing year 2015 will also contain the Device ID.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the Harney House, having purchased it for $450,000 on or about April 24, 2020. However, social media posts by ALTAMIRANO indicate the house is a rental house.

10. County property records show ALTAMIRANO and his wife, Angela ALTAMIRANO ("ANGELA") purchased PREMISES I in 2006 and ALTAMIRANO granted PREMISES I to ANGELA as her separate estate in November 2020. Nevertheless, video surveillance conducted on the SUBJECT PREMISES from February 5, 2021, through April 8, 2021, shows that ALTAMIRANO lives at PREMISES I with his wife and one daughter. During this entire surveillance period, ALTAMIRANO was observed leaving PREMISES I nearly every day in the morning and returning to PREMISES I in the evening. On days that he worked at PREMISES II, surveillance captured ALTAMIRANO leaving PREMISES I with a soft satchel that appeared to be brown in color and arriving at PREMISES II approximately 15 minutes later. ALTAMIRANO was observed bringing this satchel into PREMISES II, leaving with it at night, and bringing it with him into PREMISES I when he returned home in the evening.

11. Additional evidence also suggests ALTAMIRANO presently resides at PREMISES I. Since February 5, 2021, two vehicles were regularly observed at PREMISES I. The first, a black Toyota Tundra with Washington license plate #C27984U, is registered to ALTAMIRANO at PREMISES I. The second vehicle, a black Jeep Cherokee with Washington license plate #AVY4669, is also registered to ALTAMIRANO at PREMISES I. Comcast provides internet service for PREMISES I, and the name on the account is ALTAMIRANO.

12. Moreover, on April 28, 2020, ALTAMIRAO submitted an application for a Paycheck Protection Program ("PPP") loan and listed PREMISES I as his home address. On August 11, 2020, ALTAMIRANO submitted his application for an investment account at TD Ameritrade and listed PREMISES I as his home address. On September 14, 2020, ALTAMIRANO submitted his application for an investment account at Webull Financial LLC, and listed PREMISES I as his home address. During an undercover operation conducted at PREMISES II on March 26, 2021 (discussed in more detail

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

below), ALTAMIRANO stated that he needed his wife to bring his UPS label from his house, presumably referring to PREMISES I.

Premises II

13. ALTAMIRANO's tax preparation business operates under the name of Servicios Latinos, which is the trade name or "dba" of Integrity Investments, LLC ("Integrity Investments"). The Employer Identification Number ("EIN") for Integrity Investments is 61-1513600 and ALTAMIRANO's PTIN is P01465285. The physical address for Servicios Latinos is PREMISES II.

14. Servicios Latinos has a business website, the address of which is servicios-latinosintegrity-investments.business.site. The website lists PREMISES II as the business location. At the top of the webpage just below the business name Servicios Latinos is the phrase, "Tax Preparation in Vancouver." This is proceeded by several pictures of ALTAMIRANO and PREMISES II. Servicios Latinos also has a Facebook page which contains a picture of ALTAMIRANO sitting behind a desk. In the "About" section of the Facebook page, the PREMISES II is listed as the address for Servicios Latinos and the business is described as, "Tax specialist." This Facebook page also lists various services offered by Servicios Latinos along with applicable fees, including for business taxes ($200), state taxes ($50), federal taxes ($100), power of attorney ($100), and divorce package ($400).

15. Integrity Investments was assigned EIN 61-1513600 by the IRS in November 2006 and is listed as a single member limited liability company with ALTAMIRANO being the single member. ALTAMIRANO filed his tax years 2015 through 2019 Forms 1040 and reported the income and expenses for Integrity Investments on a Schedule C, Profit or Loss From Business, attached to each Form 1040. ALTAMIRANO has yet to file his 2020 Form 1040.

16. Since early February 2021, ALTAMIRANO has been observed regularly unlocking the doors to PREMISES II, turning on the "Open" sign, taking cigarette breaks outside PREMISES II, and otherwise remaining inside PREMISES II until

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ALTAMIRANO closed the business at night. Furthermore, dozens of clients per day were observed entering PREMISES II with papers in their hands which, based on my training and experience, I believe to be documents used in the preparation of income tax returns.

Tax Filings

17. On or about December 19, 2017, ALTAMIRANO was assessed $2,200 in tax return preparer penalties by the IRS for 2015 and 2016 Federal Income Tax returns he prepared for client RHR. The $2,200 was comprised of $2,000 for taking an unreasonable position, $100 for failure to sign the returns, and $100 for failure to furnish identifying information on the returns. RHR was assessed additional taxes of $12,802 for 2015 and $8,347 for 2016 after the returns prepared for RHR by ALTAMIRANO were audited and many of the UEBEs and Schedule C expenses were deemed false. On or about March 12, 2018, ALTAMIRANO was assessed $100 in preparer penalties by the IRS for a 2017 Federal Income Tax return he prepared for client SB. The $100 was comprised of $50 for failure to sign the return and $50 for failure to furnish identifying information on the return. SB was assessed an additional tax of $3,708 after the tax year 2017 return prepared for SB by ALTAMIRANO was audited and many of the UEBEs and Schedule C expenses were deemed false.

18. Comcast records confirm Servicios Latinos, whose subscriber address is PREMISES II, has been assigned IP address 71.59.206.246 since at least August 30, 2020. During the previously discussed March 2021 interview with the RA, ALTAMIRANO stated that in prior years he only prepared about 10-20 returns per year but this year he has prepared 40-50 returns. The IRS began accepting tax returns for tax year 2020 on February 12, 2021, and since that time at least 629 Federal Income Tax Returns have been transmitted to the IRS from IP address 71.59.206.246 but none of those returns contain ALTAMIRANO's PTIN or other required identifying information. Using video surveillance, I have identified over 100 unique license plates of people that have visited PREMISES II since February 5, 2021. To date I have identified 64

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

registered owners of these vehicles by searching the respective state Department of Licensing records. By cross-referencing the identities of these 64 registered owners with IRS records, I have determined 27 of these people have already had tax returns processed by the IRS for processing year 2021. Of these 27, 19 had returns electronically filed that contain two or more pieces of information that identify ALTAMIRANO as the return preparer, such as IP address, phone number, email address and Device ID.

19. ALTAMIRANO has filed his personal Federal Income Tax return every year for the last ten years. ALTAMIRANO claimed the Head of Household filing status in eight of those years and the Single filing status in the remaining two years. ALTAMIRANO's wife, ANGELA, has filed her personal Federal Income Tax return in eight of the last ten years. ANGELA claimed Head of Household filing status in all eight years. ALTAMIRANO listed his home address as PO Box 1601 on six of his last ten Federal Income Tax returns, and 14808 SE Rivercrest Drive on the remaining four returns. County property records indicate 14808 SE Rivercrest Drive has been owned by Belen and Steven Ortiz since 1999. ALTAMIRANO indicated on his Business Account Application with TD Ameritrade that Belen Ortiz is his mother. ANGELA listed her home address as PREMISES I on seven of her last eight Federal Income Tax returns, and 14808 SE Rivercrest Drive on the remaining return.

20. Married taxpayers have but two choices for filing status on their personal Federal Income Tax return – married filing jointly or married filing separately. Based on my training and experience I know that married taxpayers will sometimes file as unmarried to claim the Head of Household or Single filing status to qualify for higher standard deductions and Earned Income Credits ("EIC"). For example, for tax year 2018 ALTAMIRANO and ANGELA filed separate returns and each claimed Head of Household and the EIC. The standard deduction for Head of Household in 2018 was $18,000, whereas the standard deduction for married filing jointly was $24,000 (married filing separate would have resulted in an even lower standard deduction). By filing separate returns and claiming Head of Household ALTAMIRANO and ANGELA

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

inflated their total standard deduction for 2018 by taking two $18,000 ($18,000 x 2 = $36,000) standard deductions instead of the $24,000 required for married couples filing jointly. ALTAMIRANO and ANGELA used the same tactic to secure a combined EIC of $7,419 for 2018, whereas had they filed married filing jointly they would have only received approximately $2,592 (taxpayers who file married filing separate do not qualify for the EIC).

21. Furthermore, on his TD Ameritrade individual investment account application, completed August 8, 2020, ALTAMIRANO reported that he was a self-employed accountant/auditor/bookkeeper with annual income exceeding $250,000. On his Webull Financial LLC individual investment account application, completed on or about September 14, 2020, ALTAMIRANO reported that his annual income was between $500,000 and $1,200,000. Conversely, ALTAMIRANO reported total income on his tax years 2015 through 2019 personal Federal income tax returns in the following amounts, respectively: $11,668, $13,206, $11,437, $31,060, and $42,442.

PPP Loan

22. As previously mentioned, on April 28, 2020, ALTAMIRAO submitted an application for a PPP loan. As part of his PPP loan application ALTAMIRANO provided a copy of his 2019 Schedule C to Celtic that reported significantly less expenses than the 2019 Schedule C ALTAMIRANO submitted to the IRS with his 2019 Form 1040. Total business expenses on the Schedule C provided to Celtic totaled $215,820, while total business expenses on the Schedule C filed with the IRS totaled $296,033. On the Schedule C filed with the IRS, ALTAMIRANO inflated car and truck expenses by $1,213, supplies by $10,000, and rent by $69,000. County property records indicate PREMISES II is owned by Legacy Rental Properties, LLC ("Legacy"). A review of Integrity Investments' bank statements revealed that ALTAMIRANO pays Legacy $2,900 per month, or $34,800 annually. ALTAMIRANO reported rent expense of $36,000 on the Schedule C provided to Celtic, which approximates actual payments to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Legacy. However, on the Schedule C filed with the IRS ALTAMIRANO reported rent expense of $105,000.

23. ALTAMIRANO indicated on his PPP application that his was not a seasonal business and that he had monthly payroll of $12,391. IRS and Washington Employment Security Department records, however, revealed that neither ALTAMIRANO nor Integrity Investments LLC have issued a Form W-2 to an employee since at least 2015. Per IRS records, Integrity Investments has issued only three Forms 1099-MISC to independent contractors since 2015. Two Forms 1099-MISC were issued for 2015 and totaled $75,182, and one of those was issued to ANGELA for $60,041. The third Form 1099-MISC was issued for 2019 in the amount of $55,285 which, when averaged over twelve months, equates to $4,607 per month.

24. On May 4, 2020, ALTAMIRANO received a PPP loan for $30,977.

Undercover Shop

25. On March 26, 2021, an IRS-CI undercover operation was conducted at PREMISES II. One undercover agent (UCA) was sent into the office at PREMISES II to have a tax return prepared. The UCA had a Form W-2 with wages of $19,968 and $756.60 of Federal income tax withheld. Additionally, the UCA had a handwritten list of cash receipts received from house cleaning work performed as an independent contractor for which the UCA was not given a Form 1099-NEC or 1099-MISC. The total of all cash receipts was $20,496 and the UCA had no expenses related to this income. The UCA's filing status was single with zero dependents. With these parameters the correct Federal income tax due on the return was $4,769.

26. The UCA initially met with ALTAMIRANO, informing him of the need to have a tax return prepared. After a brief conversation ALTAMIRANO instructed the UCA to sit at a desk where one of his data-entry clerks would input the UCA's information into a computer. The data entry clerk took the UCA's documents, entered the information into a laptop computer, created a physical file folder for the UCA, then excused herself. After some time ALTAMIRANO sat where the data entry clerk had sat

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

and began to complete the UCA's 2020 Form 1040. ALTAMIRANO printed several forms and, after collecting them from the printer, instructed the UCA on the need to use Schedule C, Profit or Loss From Business, to report the UCA's cash receipts of $20,496. ALTAMIRANO explained to the UCA that if he reported the $20,496 in cash receipts, along with the wages reported on the UCA's Form W-2 of $19,968, the UCA would owe Federal income taxes of $4,740. ALTAMIRANO also wrote this figure on the handwritten earnings summary provided to him by the UCA, which he returned to the UCA at the end of the meeting. ALTAMIRANO further explained that if he reported only $5,000 of cash receipts, perhaps what the UCA deposited into a bank account, and claimed $7,000 in expenses the UCA would receive a refund of all Federal income taxes withheld. Lastly, ALTAMIRANO informed that UCA that if he did not report any of the cash receipts the UCA would only owe Federal income tax of $1.

27. ALTAMIRANO suggested the UCA not report the cash receipts and just pay $1 to the IRS. The UCA accepted this suggestion and ALTAMIRANO completed the return without the cash receipts. ALTAMIRANO said he would pay the $1 in Federal income tax owed by the UCA. The UCA paid ALTAMIRANO $100 cash for preparation of the 2020 Form 1040.

28. At one point towards the end of the meeting, ALTAMIRANO turned his laptop towards the UCA. The UCA was able to see that ALTAMIRANO was using Turbo Tax to prepare the UCA's income tax return. ALTAMIRANO subsequently provided the UCA with a copy of the 2020 Form 1040 he prepared. In the "Paid Preparer Use Only" section of the UCA's income tax return, on the line for "Firm's name", are two strips of white out correction tape. This is an indicator that ALTAMIRANO used either the free or consumer version of Turbo Tax and used the correction tape to cover up the "Self-Prepared" text that prints on the income tax return when using one of these products. The free and consumer versions of Turbo Tax carry the expectation that the taxpayer is self-preparing his or her return and therefore does not offer the option to enter a PTIN or any other preparer identification information.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

29. During the undercover operation at PREMISES II, ALTAMIRANO told the UCA he had to call his wife and ask her to bring his UPS label from his house. ALTAMIRANO placed the call in front of the UCA and asked the person on the end of the line to bring "my little UPS label off the kitchen counter downstairs", and also asked to bring a business card for an electrician that was, "upstairs on the chest of drawers by my little lamp." ANGELA was observed by the IRS Special Agents arriving at PREMISES II approximately sixteen minutes later. ANGELA subsequently prepared a receipt for the UCA and assembled the UCA's return copies in the previously prepared file folder.

BUSINESS AND TAX RECORDS

30. Based on my training and experience, persons engaged in tax schemes, conspiracies to defraud the United States, evasion of income tax, the filing of false returns, and obstruction of the administration of the income tax law often maintain records for long periods of time, particularly when they are involved in a pattern of conduct over a long period of time. There are many reasons why criminal offenders maintain evidence for long periods of time. The evidence may be innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, check books, videotapes and photographs, utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone and pager bills, keys to safe deposit boxes, packaging materials, computer hardware and software), but have significance and relevance when considered in light of other evidence. The criminal offender may no longer realize he still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed any computer-related evidence, which may be retrievable by a trained forensic computer expert. In addition, Title 26, United States Code, Section 6001 and the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

corresponding regulations require taxpayers keep records for no less than three years after the return is filed.

31. Based on my training and experience, persons engaged in tax schemes, conspiracies to defraud the United States, evasion of income tax, the filing of false returns, and obstruction of the administration of the income tax law, frequently retain records of their correspondence and transactions within their business and other places under their control. These records may be in the form of written communications, emails, receipts, negotiated instruments, contracts, bank statements, tax returns, and other records. Records of this kind are often also stored on computer media.

32. Based on my training and experience, I know that companies often keep their financial and business records where they conduct business. This allows the company to consult and use the information when making business decisions and preparing financial information, including for legal and regulatory purposes such as filing tax returns. Other such documents kept by companies include:

a. Banking records, such as bank statements, cancelled checks, withdrawal slips, check registers, deposit tickets, loan documents, and correspondence;

b. Income records, such as sales invoices, receipts, cash register tapes, cash receipt logs, sales journals, credit card merchant account statements and records, and customer information;

c. Expense records, such as purchase receipts, invoices, credit card statements, copies of cashier's checks, petty cash logs, journals, and ledgers of expenditures;

d. Asset acquisition and disposal records, such as titles, deeds, contracts, receipts, inventory records, invoices, and depreciation schedules;

e. Payroll records, such as employee lists, timecards, Forms W-2, Forms W-4, and records of payments;

f. Financial records, such as income statements, cash flow statements, balance sheets, bookkeeping records, and income and expense projections;

g. Tax documents, such as filed and unfiled state and federal income and excise tax returns and employment tax returns;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

h. Audit and compliance records, such as correspondence with or about audits and compliance requirements, copies of complete or incomplete financial disclosure forms, including Form 8300;

i. Regulatory and industry association information, such as guides to best practices, industry training/conference materials, rules and regulations, business and other licenses, pamphlets/notices, regulatory and compliance requirements, and correspondence with regulatory agencies; and

j. Corporate records, such as incorporation records, annual reports, stock books/ownership records, agreements, and shareholder or investor loans.

Surveillance of PREMISES II, along with records obtained and reviewed during this investigation, demonstrates that ALTAMIRANO conducts business at PREMISES II.

33. Based on my training and experience, I also know that owners of small and closely held businesses often keep personal records and documents at their place of business. These records often include personal bank records, records showing asset ownership and acquisition, investments, records of cash hoards, insurance records, loan records, promissory notes, agreements, correspondence, travel documents, safe deposit box keys, notes, and tax information.

34. Based upon my training and experience, I know that individuals and businesses commonly use computers or other electronic storage media to prepare and store the records described above and to prepare, complete, print, and file tax returns. It is likely that the records described above would be found on computers and other electronic storage media found in PREMISES I and PREMISES II for the following reasons:

a. Video from the undercover operation clearly shows ALTAMIRANO preparing the UCAs tax return on a silver Hewlett-Packard laptop computer.

b. During the undercover operation the UCA personally observed approximately nine laptop computers on desks throughout PREMISES II.

c. 629 returns identified and believed to be prepared by ALTAMIRANO were transmitted to the IRS electronically from a computer since February 5, 2021. The IRS received a Device ID as part of each transmission.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. While conducting surveillance I personally observed ALTAMIRANO sitting at a desk working on a computer while meeting with clients.

e. The website for Servicios Latinos has a "Make Appointment" link, which redirects clients to the following web address: meetings.hubspot.com/servicioslatino. At this address is a web page, hosted by Hubspot, containing a calendar for Servicios Latinos. Clients can select a date, time, and length of appointment to have their tax returns prepared and, after entering their name, email address and phone number, can click on a button to confirm this appointment.

f. The Facebook page for Servicios Latinos contains a post by Servicios Latinos with the following statement: "You can call or text (360) 443-7617 to schedule your appointment." There is also a post by Servicios Latinos encouraging clients to fax, email, or text their documents and a phone number and email address are provided.

35. Based on my training and experience, I know that these business and personal records kept where a company conducts business can be useful in showing whether a person or entity reported all income to the IRS or evaded federal tax requirements.

36. Based on my training and experience, when investigating tax crimes, I know that it is useful to compare tax and financial records maintained by a business over the course of multiple years in order to evaluate, among other things, the business' income, expenditures, and accounting practices. Based on my training and experience, companies retain business records for extended periods of time and are legally obligated to retain tax records for multiple years after a return is filed or tax is paid.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

37. As described above and in Attachment B, this application seeks permission to search for evidence, fruits and/or instrumentalities that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the evidence, fruits and/or instrumentalities might be found is data stored on digital devices, such as computer hard drives or other electronic storage media. Thus, the warrant applied for would authorize the seizure of digital devices or other electronic storage

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

media or, potentially, the copying of electronically stored information from digital devices or other electronic storage media, all under Rule 41(e)(2)(B)

38. Based upon my review of the evidence gathered in this investigation, my review of data and records, information received from other agents and computer forensics examiners, and my training and experience, I submit that if a computer or other electronic storage media is found at the SUBJECT PREMISES, there is probable cause to believe that evidence, fruits, and/or instrumentalities of the crimes of Title 26, United States Code, Sections 7206(1)-(2) (Fraud and False Statements), and Title 18, United States Code, Section 1343 (Wire Fraud) will be stored on those digital devices or other electronic storage medium, for at least the following reasons:

a. Based on actual inspection of evidence related to this investigation, such as bank statements, financial statements and emails, I am aware that computer equipment was used to generate, store, and print documents used in filing tax returns that could violate 26 U.S.C. §§ 7201 and 7206(2). There is reason to believe that there are computer systems currently located at PREMISES I and PREMISES II.

b. A review of evidence and witness statements shows ALTAMIRANO prepared returns on a computer and printed client return copies from a computer.

c. Review of evidence in this investigation shows ALTAMIRANO used the TurboTax software program from Intuit Inc. to prepare and transmit tax returns to the IRS.

d. Review of evidence in this investigation shows ALTAMIRANO entered email addresses, for accounts which he had access to, into the TurboTax software program to receive status updates on the processing of returns.

e. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

f. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

g. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation; file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

h. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

39. As further described in Attachment B to the application for PREMISES I and PREMISES II, I am seeking permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any digital device in the SUBJECT PREMISES because, based on my knowledge, training, and experience, I know:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time. Further, forensic evidence on a digital device can show how and when it was accessed or used. Such "timeline" information allows the forensic analyst and investigators to understand the chronological context of access to the digital device, its use, and events relating to the offense under investigation. This "timeline" information may tend to either inculpate or exculpate the user of the digital device. Last, forensic evidence on a digital device may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information on a digital device may indicate the user's motive and intent to commit a crime (e.g., relevant web searches occurring before a crime indicating a plan to commit the same), consciousness of guilt (e.g., running a "wiping program" to destroy evidence on the digital device or password protecting or encrypting such evidence in an effort to conceal it from law enforcement), or knowledge that certain information is stored on a digital device (e.g., logs indicating that the incriminating information was accessed with a particular program).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

40. I know that when an individual uses either a business or personal computer in keeping records the individual's business computers often will serve both as instrumentalities for committing the crime and storage media for evidence of the crime. Based on the information in this Affidavit, I believe that the digital devices belonging to ALTAMIRANO and Servicios Latinos at PREMISES I and PREMISES II are instrumentalities of crime as well as storage devices, because they constitute the means by which ALTAMIRANO committed the violations. Any personal or business computers belonging to ALTAMIRANO or Servicios Latinos at PREMISES I or PREMISES II likely were used to commit the crimes of false statements, willful aiding or assisting in the preparation of false tax returns, and wire fraud in violation of 26 U.S.C. §§ 7206(1) & 7206(2) and 18 U.S.C. § 1343 because they were used by ALTAMIRANO (a) to prepare client tax returns; (b) collect payments for the business; (c) to discuss services with clients through email and other communications; (d) to post information to the website and social media accounts of the businesses. Therefore, I believe that in addition to seizing the digital devices to conduct a search of their contents as set forth herein, there is probable cause to seize those digital devices as instrumentalities of the criminal activity.

41. If, after conducting its examination, law enforcement personnel determine that any digital device is any instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture. If law enforcement personnel determine that a device was not an instrumentality of the criminal offenses referenced above, it shall be returned to the person/entity from whom it was seized within 90 days of the issuance of the warrant, unless the government seeks and obtains authorization from the Court for its retention.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PAST EFFORTS TO OBTAIN ELECTRONICALLY STORED INFORMATION

42. Because of the nature of the evidence that I am attempting to obtain and the nature of the investigation, I have not made any prior efforts to obtain the evidence based on the consent of any party who may have authority to consent. I believe, based upon the nature of the investigation and the information I have received, that if ALTAMIRANO becomes aware of the search warrant, he may attempt to destroy any potential evidence, whether digital or non-digital, thereby hindering law enforcement agents from the furtherance of the criminal investigation.

RISK OF DESTRUCTION OF EVIDENCE

43. I know, based on my training and experience, that digital information can be very fragile and easily destroyed. Digital information can also be easily encrypted or obfuscated such that review of the evidence would be extremely difficult, and in some cases impossible. I do not know whether, in the instant case, ALTAMIRANO used encryption on the computer systems he utilizes to engage in his crimes. If an encrypted computer is either powered off, or if the user has not entered the encryption password and logged onto the computer, it is likely that any information contained on the computer will be impossible to decipher. If the computer is powered on, however, and the user is already logged onto the computer, there is a much greater chance that the digital information can be extracted from the computer. This is because when the computer is on and in use, the password has already been entered and the data on the computer is accessible. However, giving the owner of the computer time to activate a digital security measure, pull the power cord from the computer, or even log off of the computer, could result in a loss of digital information that could otherwise have been extracted from the computer.

REQUEST FOR AUTHORITY TO CONDUCT OFF-SITE SEARCH OF TARGET COMPUTERS AND OTHER DIGITAL DEVICES

44. In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. *The time required for an examination*. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. *Technical requirements*. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. *Variety of forms of electronic media*. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

SEARCH TECHNIQUES

45. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit seizing, imaging, or otherwise copying digital devices or other electronic storage media that reasonably appear capable of containing some or all of the data or items that fall within the scope of Attachment B to the application seeking authorization to search PREMISES I and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PREMISES II, and will specifically authorize a later review of the media or information consistent with that warrant.

46. Consistent with the above, I am requesting the authority to seize and/or obtain a forensic image of digital devices or other electronic storage media that reasonably appear capable of containing data or items that fall within the scope of Attachment B to the application seeking authorization to search PREMISES I and PREMISES II, and to conduct off-site searches of the digital devices or other electronic storage media and/or forensic images, using the following procedures:

a. Upon securing the physical search site, the search team will conduct an initial review of any digital devices or other electronic storage media located at PREMISES I or PREMISES II described in Attachment A that are capable of containing data or items that fall within the scope of Attachment B to this Affidavit, to determine if it is possible to secure the data contained on these devices onsite in a reasonable amount of time and without jeopardizing the ability to accurately preserve the data.

b. In order to examine the electronically stored information ("ESI") in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of any digital device or other electronic storage media that is capable of containing data or items that fall within the scope of Attachment B.

c. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the subject device. Creating an image of the devices located at the search location described in Attachment B will not result in access to any data physically located elsewhere. However, digital devices or other electronic storage media at the search location described in Attachment A that have previously connected to devices at other locations may contain data from those other locations.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. In addition to creating an image of a physical or logical drive from a digital device or other electronic storage media, law enforcement may attempt to create an image of the random access memory ("RAM") of a digital device. Agents may only create an image of a digital device's RAM if the computer is powered on at the time of the search. This is because RAM is only active when the device is in operation. Any data contained in the RAM will be lost when the computer is powered off. A computer's RAM may contain evidence related to who else is logged onto the computer (even remotely), open connections that might indicate a program is waiting for commands, passwords for encryption programs, hardware and software settings, maps of recent files and applications accessed, and information related to what communication vendors have recently been utilized on the device (i.e. instant messaging services, e-mail services, social networking sites, etc.). In addition, RAM may contain encryption keys necessary to access other elements of the subject device.

e. If based on their training and experience, and the resources available to them at the search site, the search team determines it is not practical to make an on-site image within a reasonable amount of time and without jeopardizing the ability to accurately preserve the data, then the digital devices or other electronic storage media will be seized and transported to an appropriate law enforcement laboratory to be forensically imaged and reviewed.

f. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. Those techniques, however, may necessarily expose many or all parts of a hard drive to human inspection in order to determine whether it contains evidence described by the warrant.

47. The following filter team protocol will be used for digital devices:

a. A filter team will conduct the copying and review of digital devices, and any forensic images thereof, that are seized pursuant to Rule 41(e)(2)(B) of the Federal Rule of Criminal Procedure. The filter team will perform an initial review of the original device or image within a reasonable amount of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to determine whether the device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant.

b. After conducting its review, the filter team will create a "results copy" of the evidence that contains only those items of evidence that law enforcement is authorized to seize pursuant to Attachment B. The filter team will transmit the results copy to the case agents, investigators, and prosecutors assigned to the investigation ("the prosecution team"). The filter team will operate independently from the prosecution team.

c. If, after conducting the initial search, the filter team determines that the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search not to exceed 120 days from the date of execution of the warrant unless an extension is authorized by the Court.

d. Digital devices that constitute instrumentalities of the crimes identified in Attachment B may be maintained for the purpose of preserving evidence for trial, ensuring the chain of custody, and litigating any issues of forfeiture. The digital devices, or forensic images thereover, cannot, be further searched absent another search warrant.

e. The prosecution team will make available to the defense a copy of the forensic image of any seized digital device that is maintained by the government provided that the image does not contain contraband.

f. The filter team will employ only those methodologies, techniques and protocols that may reasonably be expected to find, identify, segregate and/or duplicate the items that law enforcement is authorized to seize pursuant to Attachment B of the warrant. If the filter team, during its examination, comes across in plain view evidence of criminal activity constituting an offense that is not identified in Attachment B, the filter team may alert the U.S. Attorney's Office so an evaluation can be made as to what additional action may be taken such as applying for a search warrant to broaden the scope of the examination.

REQUEST FOR SEALING

48. It is respectfully requested that the Court issue an order sealing, until further order of the Court, all papers submitted in support of the requested search

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

warrants, including the application, this affidavit, the attachments, and the requested search warrants. I believe that sealing these documents is necessary because the information to be seized is relevant to an ongoing investigation, and disclosure of these materials at this time will jeopardize the progress of the investigation by giving the subject of the investigation an opportunity to destroy evidence, change patterns of behavior, or flee from prosecution.

CONCLUSION

49. Based upon the evidence set forth herein, I respectfully submit that there is probable cause to believe that KEITH MARK ALTAMIRANO made false statements on his tax returns, prepared false tax returns, and committed wire fraud in violation of Title 26, United States Code, Section 7206(1) (False and Fraudulent Statements by Taxpayer), Title 26, United States Code, Section 7206(2) (Aiding False and Fraudulent Statements by Third Parties), and Title 18, United States Code, Section 1343 (Wire Fraud), and that evidence, contraband, fruits, and instrumentalities of those offenses, as described above and in Attachment B, are presently located at PREMISES I and PREMISES II, which are described in Attachments A-1 and A-2, respectively. I therefore request that the Court issue warrants authorizing a search of PREMISES I, described in Attachment A-1, and

XX

XX

XX

XX

XX

XX

XX

XX

XX

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PREMISES II, described in Attachment A-2, for the items listed in Attachment B and the seizure and examination of any such items found.

Respectfully submitted,

Christian D. Martin

CHRISTIAN D. MARTIN, Affiant
Special Agent
IRS Criminal Investigation

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 15th day of April, 2021.

J. Richard Creatura

J. RICHARD CREATURA
Chief United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1
Property to be Search

The property to be searched is 7914 SE Evergreen Highway, Vancouver, WA 98664 ("PREMISES I"), further described as a split-level single-family residence. PREMISES I is painted light blue with darker blue trim. The main entrance to PREMISES I faces south and is comprised of two wood doors, brown in color, with glass inlays. The main entrance can be accessed by climbing a set of approximately six wooden stairs. There is an approximately six-foot high iron fence on the south side of the property. The fence contains a pedestrian gate on the west end and a double-car gate just east to the pedestrian gate. The fence is comprised of pickets and the double-car gate has symmetrical, intricate designs of deer and mountains on each side.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2
Property to be Search

The property to be searched is 3312 E Fourth Plain Boulevard, Suites 110 & 115, Vancouver, WA 98661, further described as two offices located on the northwest corner of a single-story commercial building on the north side of E Fourth Plain Boulevard approximately 100 yards west of the intersection of E Fourth Plain Boulevard and Neals Lane. The building is painted a light brown, or tan, color. There are two additional businesses, Elvia's Hair Salon and Recovery Café, located in the same building. The Subject Premises occupies two offices, or suites, in this building and the other businesses are not accessible from within the suites of Subject Premises. The Subject Premises can only be accessed from the west side via two glass doors clearly marked with suite numbers 110 and 115. The Subject Premises has a white sign with black lettering and trim above the glass doors that reads, in part:

SERVICIOS LATINOS

Exito en la Comunidad Latina · 360-433-7617

Inside the Subject Premises are two suites. Suite 110 is on the right and suite 115 is on the left. An interior doorway connects the two suites approximately midway of the dividing interior wall. Suite 110 contains a client lobby, receptionist desk, and desks for

XX

XX

XX

XX

XX

XX

XX

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

data entry clerks to meet with clients. Suite 115 contains a desk on the front-left side, an enclosed office in the middle-left, and another desk in the back-left. A walkway runs along the right side of suite 115.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B
Items to be Seized

This warrant authorizes the government to search for the following evidence, fruits and/or instrumentalities of Title 26, United States Code, Section 7206(1) (False and Fraudulent Statements by Taxpayer), Title 26, United States Code, Section 7206(2) (Aiding False and Fraudulent Statements by Third Parties), and Title 18, United States Code, Section 1343 (Wire Fraud) for the time period January 1, 2015 through the present, whether recorded on paper or stored electronically on computers and related peripheral devices:

Records, Documents, and Items

1. All bank account records, checking, savings account, investment accounts, bonds, certificates of deposits, signature cards, wire transfers, EFT deposit and withdrawal information, deposit receipts, wire transfers, money orders, loan documents, loan applications, loan payment records, official checks, foreign accounts in any foreign or domestic financial institution and any other related financial documents;
2. All loan records, including loan applications, promissory notes, records reflecting receipt of loan funds, loan balance records, loan statements, loan repayment schedules, loan balance records, and correspondence regarding loans;
3. All credit card records, including credit card applications, credit card statements, credit card payment records, records of items purchased with credit cards; correspondence regarding credit cards;
4. Account ledgers, journals, logs, balance sheets, receipts or papers showing personal and business income; account ledgers, journals, logs, balance sheets receipts or papers showing personal and business expenses, sales invoices, sales receipts, expense invoices, balance sheets;
5. Diaries of business activities, calendars, telephone records, payroll records, employment records, business planners;
6. Documents and records relating to the preparation or filing of federal or state income tax returns including any individual, corporate, partnership, trust, and employer state and federal income tax returns, schedules, Forms W-2, Form 1040X, Forms W-4, Forms 1099, Forms 1041, Forms K-1, notices and correspondence with the IRS and other taxing authorities, client lists and contact information, work papers, and tax preparation materials;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

7. Records, documents, receipts, books, files, correspondence, other articles or information relevant to the computation of the federal income tax liability of Keith Mark Altamirano (aka Larry Altamirano) or Integrity Investments, LLC., dba Servicios Latinos from January 1, 2015 to the date of the execution of the warrant;

8. Documents or materials related to training in tax law and/or the preparation of tax returns, including training manuals, examples, templates, and correspondence in electronic, video, and paper formats;

9. Any safe or locked receptacle or compartment, in which some or all of the property mentioned may be maintained; and

10. Records relating to the purchase or sale of assets such as stocks, real estate, vehicles, securities, jewelry, recreational vehicles, boats, and aircraft by Keith Mark Altamirano (aka Larry Altamirano) or Integrity Investments, LLC., dba Servicios Latinos.

Digital Evidence

1. Digital devices[1] or other electronic storage media[2] and/or their components devices used as a means to commit the violations described above, which include:

   A. Any digital device or other electronic storage media capable of being used to commit, further, or store evidence of the offenses listed above;

   B. Any digital devices or other electronic storage media used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, plotters, encryption devices, and optical scanners;

   C. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

---

[1] "Digital device" includes any device capable of processing and/or storing data in electronic form, including, but not limited to: central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants ("PDAs"), iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), or portable media players.

[2] Electronic Storage media is any physical object upon which electronically stored information can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

D. Any documentation, operating logs and reference manuals regarding the operation of the digital device or other electronic storage media or software;

E. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

F. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

G. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

2. For any digital device or other electronic storage media upon which electronically stored information that is called for by this warrant may be contained, or that may contain things otherwise called for by this warrant:

A. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

B. Evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

C. Evidence of the lack of such malicious software;

D. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

E. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

F. Evidence of the times the digital device or other electronic storage media was used;

G. Passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

H. Documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media; and

I. Contextual information necessary to understand the evidence described in this attachment.

3. Records and things evidencing the use of an Internet Protocol address 71.59.206.246 to communicate with the internet service provider or other network, including:

A. Routers, modems, and network equipment used to connect computers to the Internet;

B. Records of Internet Protocol addresses used; and

C. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

Filter Team Protocol for Digital Devices

1. A filter team will conduct the copying and review of digital devices, and any forensic images thereof, that are seized pursuant to Rule 41(e)(2)(B) of the Federal Rule of Criminal Procedure. The filter team will perform an initial review of the original device or image within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to determine whether the device or image contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant

2. After conducting its review, the filter team will create a "results copy" of the evidence that contains only those items of evidence that law enforcement is authorized to seize pursuant to Attachment B. The filter team will transmit the results copy to the case agents, investigators, and prosecutors assigned to the investigation ("the prosecution team"). The filter team will operate independently from the prosecution team.

3. If, after conducting the initial search, the filter team determines that the digital device does not contain any data falling within the ambit of the warrant, the government will return the digital device to its owner within a reasonable period of time following the search not to exceed 120 days from the date of execution of the warrant unless an extension is authorized by the Court.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

4. Digital devices that constitute instrumentalities of the crimes identified in Attachment B may be maintained for the purpose of preserving evidence for trial, ensuring the chain of custody, and litigating any issues of forfeiture. The digital devices, or forensic images thereover, cannot, be further searched absent another search warrant.

5. The prosecution team will make available to the defense a copy of the forensic image of any seized digital device that is maintained by the government provided that the image does not contain contraband.

6. The filter team will employ only those methodologies, techniques and protocols that may reasonably be expected to find, identify, segregate and/or duplicate the items that law enforcement is authorized to seize pursuant to Attachment B of the warrant. If the filter team, during its examination, comes across in plain view evidence of criminal activity constituting an offense that is not identified in Attachment B, the filter team may alert the U.S. Attorney's Office so an evaluation can be made as to what additional action may be taken such as applying for a search warrant to broaden the scope of the examination.

THE SEIZURE OF DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA AND/OR THEIR COMPONENTS AS SET FORTH HEREIN IS SPECIFICALLY AUTHORIZED BY THIS SEARCH WARRANT, NOT ONLY TO THE EXTENT THAT SUCH DIGITAL DEVICES OR OTHER ELECTRONIC STORAGE MEDIA CONSTITUTE INSTRUMENTALITIES OF THE CRIMINAL ACTIVITY DESCRIBED ABOVE, BUT ALSO FOR THE PURPOSE OF THE CONDUCTING OFF-SITE EXAMINATIONS OF THEIR CONTENTS FOR EVIDENCE, INSTRUMENTALITIES, OR FRUITS OF THE AFOREMENTIONED CRIMES

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970